Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of:	)	
	)	
Interoperability, Out of Band Emissions,	)	PS Docket No. 06-229
and Equipment Certification for 700 MHz	)	
Public Safety Broadband Networks,	)	
DA 10-884	)	

Comments of IPWireless, Inc.

Introduction

IPWireless, as a supplier of 3GPP standards-based technology to public safety mobile broadband networks, is pleased to submit the following comments on this proceeding.

In our comments below, the questions posed by the Commission are summarized in italics, and IPWireless comments in plain text.

IPWireless understands that the purpose of the waivers is to allow the early deployment of public safety mobile broadband networks to allow agencies to meet immediate operational needs and gain experience with the deployment and operation of such networks, including the gathering of traffic statistics that will assist in determining the spectrum requirements for public safety. Small LTE networks can be easy to deploy and operate, however 3GPP release 8 LTE can be a complex and difficult architecture to deploy if the full range of inter-network interfaces and services are required in systems operating under waivers, especially where the relevant standards (such as for voice) and commercial band 14 products are not yet ready. Mandating an extensive range of requirements could delay the deployment of waiver networks, and in doing so defeat the purpose of the waivers.

Interoperability

Applications

Are applications specified in National Public Safety Telecommunications Council's Broadband Task Force Report (NPSTC BBTF Report) sufficient for the purpose of promoting nationwide interoperability?

Some of these applications may rely on the further development of standards. We seek comment on the availability and timeliness of the standards development process and what standard conformance we should require to achieve interoperability. How can we ensure requirements are met through our rules, while still recognizing the need for technical evolution?

For systems operating under waivers, we suggest that the minimum application requirements be (a) Internet Access, (b) VPN access to the roamer's home network, (c) a status / messaging home page on the visited network and (d) access to Incident Command System applications on the visited network (limited to those applications using generic IP access). Mandatory requirements for other applications may delay the deployment of networks under waivers, especially those that require further standards development or extensive agreements between jurisdictions operating waiver networks.

Roaming

The Waiver Order requires two types of roaming categories that would allow users of one public safety network to roam to another public safety network. We seek comment on any additional roaming requirements, such as handoff between public safety networks especially in case of regional emergencies. We seek comment on whether there would be any technical ramifications requiring rule changes for the operation of public safety networks should the Commission decide to allow roaming to and from commercial networks.

As roaming requires agreements between jurisdictions, implementation of roaming interfaces, and clearing house arrangements which may take time for the public safety community to put in place, IPWireless proposes that roaming only be required between waiver cities/ counties which are immediately adjacent, within the same metropolitan area, or elsewhere by mutual agreement where there is a specific need.

While handoff of sessions in progress between overlapping networks is always desirable, in a packet based system such as LTE where voice is not initially supported, cell reselection onto the roaming network can be acceptable for many applications. By not requiring handover between waiver networks of different jurisdictions, the Commission can facilitate early deployments by not requiring the implementation of the core network interfaces required for roaming and the coordination of engineering for coverage overlap and neighbor lists.

System Characteristics, Interfaces and Testing.

We seek comments on the requirements set in the Waiver Order for use as a basis for the final FCC rules. Is the self-certification sufficient to ensure the Interoperability Testing (IOT) requirement on a long term basis? If not, what other mechanisms should be implemented? Similarly, if standards conformance testing as specified in the Waiver Order is not fully available in a timely manner, what other mechanisms should be implemented?

Interoperability testing and standards conformance certification for an advanced wireless standard such as 3GPP LTE is a complex process. The test cases are prepared by 3GPP, the tests are then implemented and proven by test system manufacturers, following which user devices can be tested for standards compliance against these test systems. Several hundred tests are required. Devices are then certified by the Global Certification Forum (GCF), and the PCS Type Certification Review Board (PTCRB) for the US market. Any shortcutting of this process can risk equipment not being fully interoperable. Therefore, self-certification cannot be assumed to ensure interoperability, so this may not be a viable option.

Regarding the selection and use of network identification numbers, the NPSTC BBTF Report notes that there are two alternatives for assigning network identification numbers to the regional networks. (1) use a single Public Land Mobile Network (PLMN) identifier for all of public safety, and use a secondary identifier (sub ID) for each individual regional network, or (2) use a different PLMN identifier for each regional network

At this early stage for public safety mobile broadband networks, it is important not to predetermine the future commercial model through inadvertently making technical requirements that favor one model over another. The use of a single PLMN identifier could result in a single national core network and favor commercial operators, reducing options and flexibility of waiver system operators, and potentially delay deployments under waivers. We believe that innovative approaches to solving the problem may exist, and IPWireless suggests that ERIC investigate all potential options to maximize flexibility for public safety operators.

Performance, Reliability, Capacity and Coverage.

The Waiver Order does not address the performance, reliability, capacity or coverage of public safety wireless broadband networks. How, if at all, do such operability parameters affect interoperability? Does a "network of networks" with different operability criteria at various parts hinder nationwide interoperability? Is service ubiquity important for public safety across all networks? For example, would it be important if performance and reliability of public safety service allowed 256 Kbps at the cell edge in one network, but only 128 Kbps in another network? Or similarly, would it be important if variances in capacity and coverage across regional networks created disparities of service throughout the nation? On the other hand, would the benefits of local control over these matters outweigh the benefits of service ubiquity and transparency?

From our experience, requirements of public safety agencies for mobile broadband differ widely, depending on the types of area to be covered, the applications to be supported, and the number of

public safety users. We therefore suggest that it would therefore be a mistake to dictate performance requirements on a national basis, as doing so may render mobile broadband networks unaffordable for some cities and counties. For example, doubling the minimum cell edge data rate increases the cell count for a given coverage area, and therefore the network cost by approximately 50%.

A public safety agency would normally deploy a network to meet its local needs and budget constraints. By definition, the level of service chosen by the local agency should be acceptable for inbound roaming users, for example in a mutual aid scenario. We suggest that local control over service levels should be allowed; there is not one size that fits all.

Nationwide Core

The Waiver Order requires the use of LTE and the associated "Evolved Packet Core" (EPC) for each public safety regional network. However, the order does not address a whether there should be a nationwide core to which all the individual networks would be connected and assumes connection to Internet as a minimum for the purpose of interconnectivity and roaming. We seek comment on whether there should be a nationwide core created for the purpose of achieving a nationwide interoperable broadband network for public safety.

We suggest that it is too early to determine whether a single nationwide core network is the best option for public safety or not. Regardless, it should not be a requirement for waiver networks, as this could predetermine the longer term outcome. The time it would take to agree upon and implement a nationwide core could also delay waiver deployments.

An important benefit of the choice of a 3GPP standard for public safety broadband is the inherent roaming and interoperability supported by the standards, which have developed out of the requirement for national and international roaming by commercial operators. The LTE standard provides the flexibility required for an interconnected "network of networks", therefore there is no significant technical justification for a single nationwide core.

In considering a nationwide core, consideration should also be given to the reliability of the network that is reliant on long distance transmission in the event of a major natural disaster or war.

Out-of-Band Emissions (OOBE)

We recognize that 3GPP Release 8 Long Term Evolution (LTE) has requirements to enable coexistence in the same geographical area and co-location between operators on adjacent channels, and that it includes other co-existence and interworking specifications. In the Waiver Order, the Commission specified 43 + 10logP dB as the OOBE limit for operations in the PSBB Block. We seek comment on the benefits of this specification, or of any proposed alternative specification, for the public safety broadband network in protecting and promoting the use of both the PSBB Block and the D Block and minimizing interference.

As the 700 MHz allocations for public safety broadband and the D Block are paired channels for frequency division duplex operations, the coexistence (and interference) issues are similar to other paired bands such as 850 MHz CMRS and 1900 MHz PCS. The primary coexistence issue is between the D block base station transmit and the public safety broadband user equipment (UE) receive in immediately adjacent spectrum. In this scenario, adjacent channel interference and / or blocking in the UE receiver will only occur when the public safety user is physically close to a D block base station while at the same time distant from its host public safety base station. Where the public safety and D block base stations are collocated, this potential interference is inherently mitigated. Alternatively, more stringent transmitter emission mask requirements could be implemented on the D Block base stations to protect D Block UE's if necessary (and conversely on public safety broadband base stations). A precedent for this exists in the Commission's emission rules for the EBS / BRS band in 47 CFR 27.53.

Equipment Certification

In the Waiver Order, the Commission waived the equipment certification requirements under Section 90.203 of the rules and required the manufacturers to comply with the various technical requirements of 3GPP Release 8

What impact will any changes in the Commission rules have on the equipment that may be deployed for operations in the PSBB Block prior to the adoption of final rules? What alternative approach would vendors and authorized network operators propose to minimize the impact in the field deployed equipment, for continued interoperability, prior to the adoption of final rules?

Any changes to the commission rules that require changes in the 3GPP standards will need to be proposed as Study Items in the 3GPP standards organization, and become part of the 3GPP work plan. This is likely to mean that changes required by the Commission may not be standardized until at least Release 10.

As the IPWireless equipment uses software defined radio (SDR) architectures, many potential changes can be implemented by software upgrade to deployed equipment. However changes to physical layer requirements such as transmitter emission masks could require hardware changes.

How do the licensees and manufacturers plan to address the continued evolution of the 3GPP standard from Release 8 LTE to future 3GPP releases? How should the Commission address this?

IPWireless implements a software defined radio architecture on its eNodeB base station and UE, as do some other LTE vendors. This allows Release 9 and potentially later release features to be implemented through software upgrade, as the 3GPP plan for enhancement of the LTE standards is known through to and including release 9. As the baseband and CPU processing power in typical eNodeB and UE hardware is in excess of that required through release 9, it is likely that subsequent releases can be implemented through software upgrade, but cannot be guaranteed until the 3GPP work plan beyond release 9 is clear.

It is common practice within the wireless industry for a network operator to qualify user devices and other equipment that will be used on its network to ensure compatibility with industry standards as specifically applied within its network. Some network operators support 3rd party service providers and equipment manufacturers with technical programs to adapt their devices to the operator's network. Should the Commission require that public safety network operators avail themselves of these processes to ensure mobile devices selected for public safety use will operate not only on public safety networks but be able to roam onto specific commercial carrier networks as well? If so, what criteria should be used to select which commercial networks equipment should be qualified for use on?

The 3GPP / GCF and PTCRB certification processes are designed to ensure wide interoperability, and therefore "private" UE qualification on networks should not be essential for normal interoperability, and could be argued as defeating the purpose of adopting a widely supported international standard.

Respectfully submitted,

IPWireless, Inc.

By: Roger P. Quayle

Chief Technology Officer

90 New Montgomery St, Suite 315, San Francisco, CA 94105